

GRÖBNER BASES OF SYMMETRIC IDEALS

STEFAN STEIDEL

ABSTRACT. In this paper we present a new algorithm to compute the Gröbner basis of an ideal that is invariant under certain permutations of the ring-variables. Furthermore, we introduce a second algorithm which is a modification of the modular computation of Gröbner bases as introduced by Idrees, Pfister, Steidel (cf. [IPS11]) in the symmetric case. In fact, the algorithm that uses the given symmetry, improves the modular calculations in positive characteristic. In particular, we could, for the first time, compute the Gröbner basis of the famous ideal of *cyclic 9-roots* (cf. [BF91]) over the rationals with SINGULAR. Both new algorithms are implemented in SINGULAR.

1. INTRODUCTION

Computing the Gröbner basis of an ideal is a powerful tool in commutative algebra, with applications in algebraic geometry and singularity theory. The first general algorithm was proposed by B. Buchberger in 1965 (cf. [Bu65]). Within this article we improve the computation of Gröbner bases in case that the input ideal has some special symmetry-character. Consider, for example, the ideal $I := \langle x^2y^2 - z, xy - 2y + 3z, xy - 2x + 3z \rangle \subseteq \mathbb{Q}[x, y, z]$. Then I does not vary if one interchanges the variables x and y , and we say that I is *symmetric* with respect to the permutation $x \longleftrightarrow y$. In the following we use this property to manipulate the ideal by an appropriate linear transformation and apply Buchberger's algorithm subsequently. We start in Section 2 by presenting some basic notations, definitions and results. In Section 3 we introduce the symmetric Gröbner basis algorithm, and state a theoretical result that reserves the impact of the symmetry in Proposition 3.8. Section 4 combines the symmetric algorithm of Section 3 with modular methods. Examples and timings are presented in Section 5.

2. BASIC NOTATIONS AND DEFINITIONS

Let $\sigma \in \mathbb{S}_n := \text{Sym}(\{1, \dots, n\})$ be a permutation. The *order* of σ is the minimal natural number $k \in \mathbb{N}_{>0}$ such that $\sigma^k = \text{id}$, in particular $\text{ord}(\sigma) := \#(\langle \sigma \rangle) < \infty$. In order to describe σ properly, we make use of the following well-known result concerning the representation of permutations.

Definition 2.1. Let $\sigma \in \mathbb{S}_n$ be a permutation. Then there exists a natural number $\vartheta(\sigma)$ and a finite disjoint partition $\{1, \dots, n\} = \coprod_{i=1}^{\vartheta(\sigma)} \{e_{i,1}, \dots, e_{i,l_i}\}$ such that

$$\sigma = (e_{1,1} \dots e_{1,l_1}) \cdots (e_{\vartheta(\sigma),1} \dots e_{\vartheta(\sigma),l_{\vartheta(\sigma)}})$$

Date: January 30, 2012.

Key words and phrases. Gröbner bases, symmetry, modular computation, parallel computation.

with $l_1 + \dots + l_{\vartheta(\sigma)} = n$ and $0 \leq l_i \leq n$ for all $i \in \{1, \dots, \vartheta(\sigma)\}$. The cycles $(e_{i,1} \dots e_{i,l_i})$ are up to alignment uniquely determined, and we call this representation the *cycle decomposition* of σ . The tuple $(l_1, \dots, l_{\vartheta(\sigma)})$ is called the *cycle type* of σ if $l_1 \leq \dots \leq l_{\vartheta(\sigma)}$.

Note that having the cycle decomposition of a permutation σ it holds $\text{ord}(\sigma) = \text{lcm}(l_1, \dots, l_{\vartheta(\sigma)})$. From now on we assume that all considered permutations $\sigma \in \mathbb{S}_n$ are given in cycle decomposition.

Now let K be a field and $X := \{x_1, \dots, x_n\}$ be a set of indeterminates, then $\sigma \in \mathbb{S}_n$ induces a canonical automorphism on the polynomial ring over K in these indeterminates, $K[X]$, via $\varphi_\sigma : K[X] \longrightarrow K[X]$, $x_i \mapsto x_{\sigma(i)}$. By abuse of notation we always write σ instead of φ_σ , i.e. we identify the group \mathbb{S}_n as a subgroup of the automorphism group $\text{Aut}(K[X])$.

Definition 2.2. Let $I \subseteq K[X]$ be an ideal and $\sigma \in \text{Aut}(K[X])$ be an automorphism. Then I is called σ -*symmetric* if $\sigma(I) = I$. Moreover, let $\mathcal{S} \subseteq \text{Aut}(K[X])$ be a subgroup then we call I \mathcal{S} -*symmetric* if it is σ -symmetric for all $\sigma \in \mathcal{S}$.

Every subgroup of \mathbb{S}_n has only finitely many elements and is therefore finitely generated. Hence, let $\mathcal{S} = \langle \sigma_1, \dots, \sigma_m \rangle \subseteq \mathbb{S}_n$ then an ideal $I \subset K[X]$ is \mathcal{S} -symmetric if and only if it is σ_i -symmetric for all $i \in \{1, \dots, m\}$. In particular, if an ideal is σ -symmetric then it is $\langle \sigma \rangle$ -symmetric.

Moreover, given an ideal $I \subseteq K[X]$ we can always choose a finite set of polynomials $F_I = \{f_1, \dots, f_r\}$ such that $I = \langle F_I \rangle$. Thus, if I is σ -symmetric with $\sigma \in \text{Aut}(K[X])$ we even may assume that $\sigma(F_I) = F_I$ by possibly adding some polynomials to F_I .

Example 2.3. The ideal $I = \langle x^2y^2 - z, xy - 2y + 3z, xy - 2x + 3z \rangle \subseteq \mathbb{Q}[x, y, z]$ is obviously σ -symmetric for $\sigma = (12)(3) \in \mathbb{S}_3$.

We denote by $\text{Mon}(X)$ the set of monomials. Moreover, if $>$ is a monomial ordering and $f \in K[X]$ a polynomial, then we denote by $\text{LC}(f)$ the leading coefficient of f , by $\text{LM}(f)$ the leading monomial of f , by $\text{LT}(f)$ the leading term (leading monomial with leading coefficient) of f , and by $\text{tail}(f) = f - \text{LT}(f)$ the tail of f with respect to the ordering $>$. In particular, with our notation it holds $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$.

Convention 2.4. In the following $>$ is a degree ordering, and we always consider reduced Gröbner bases G , that is $0 \notin G$, $\text{LM}(g) \nmid \text{LM}(f)$ for any two elements $f \neq g$ in G , and $\text{LC}(g) = 1$ respectively no monomial of $\text{tail}(g)$ is contained in the leading ideal of G for any $g \in G$.

3. COMPUTING GRÖBNER BASES USING SYMMETRY

Within this section we describe how to achieve an improvement of the Gröbner basis computation of a σ -symmetric ideal $I \subseteq K[X]$ by using its symmetric property. The basic idea is the construction and usage of an appropriate linear transformation $\tau \in \text{Aut}(K[X])$ which “diagonalises” σ and respects the σ -symmetry of I . It turns out that in many cases the usual Gröbner basis computation on the transformed side is much faster than the computation on the original side. Since the pull back of this Gröbner basis is in general not a Gröbner basis anymore we have to add another Gröbner basis computation. Nevertheless, this indirection effects an

enormous speed up compared to the usual Gröbner basis algorithm (cf. Section 5). We assume that the tuple (σ, K) with $\text{ord}(\sigma) = k \in \mathbb{N}$ always satisfies $\text{char}(K) \nmid k$ and K has a k -th primitive root of unity ξ_k .

Remark 3.1. We can always achieve this assumption by possibly adjoining ξ_k . In particular, we can swap to $K[\xi_k]$ by working over the field $K[a]/\Phi_k(a)$ where $\Phi_k(a)$ is the k -th cyclotomic polynomial.

We start by illuminating the basis for the symmetric Gröbner basis algorithm from a character theoretical point of view and in terms of linear algebra.

Therefore, we consider the n -dimensional K -subvector space $V = \langle x_1, \dots, x_n \rangle_K$ of the infinite-dimensional K -vector space $K[X]$. Then due to our assumption that $\text{char}(K) \nmid \#(\langle \sigma \rangle)$, character theory guarantees that every representation of $\langle \sigma \rangle \subseteq \mathbb{S}_n$ is a direct sum of irreducible representations (cf. [Se96, Theorem 2]), and all irreducible representations of $\langle \sigma \rangle \subseteq \mathbb{S}_n$ have degree 1 since $\langle \sigma \rangle \subseteq \mathbb{S}_n$ is an abelian group (cf. [Se96, Theorem 9]). In particular, the representation $\rho: \langle \sigma \rangle \rightarrow \text{Aut}(V)$ is diagonalisable, i.e. $V = \bigoplus_{i=1}^n V_i$ with $V_i = \langle y_i \rangle_K$ and $\rho(\sigma)(y_i) = \xi_k^{\nu_i} \cdot y_i$ for some $0 \leq \nu_i \leq k-1$.

In terms of linear algebra we have the following quite simple proposition which, together with its proof, forms the basis of the symmetric Gröbner basis algorithm.

Proposition 3.2. *Let $\sigma \in \mathbb{S}_n$ have cycle type $(l_1, \dots, l_{\vartheta(\sigma)})$. Then $\sigma \in \text{Aut}(V)$ is diagonalisable with eigenvalues $\{\xi_k^{(k/l_m)j} \mid 1 \leq m \leq \vartheta(\sigma), 0 \leq j \leq l_m - 1\}$.*

Proof. Let $\sigma = (e_1 \dots e_n) \in \mathbb{S}_n$ with $\{e_1, \dots, e_n\} = \{1, \dots, n\}$ be an n -cycle. The columns of the representation matrix $M(\sigma, X)$ of $\sigma \in \text{Aut}(V)$ with respect to the K -basis $X = \{x_1, \dots, x_n\}$ of V are just the permuted unit vectors of K^n . Hence, $M(\sigma, X)$ is a unitarian matrix and in particular diagonalisable. Moreover, let $C = t\mathbb{1}_n - M(\sigma, X) \in \text{Mat}(n \times n, K[t])$ then the characteristic polynomial of $\sigma \in \text{Aut}(V)$ is

$$\begin{aligned} \chi_\sigma = \det(C) &= \sum_{\pi \in \mathbb{S}_n} \text{sign}(\pi) \cdot c_{1\pi(1)} \cdots c_{n\pi(n)} \\ &= t^n + \text{sign}(\sigma) \cdot (-1)^n = t^n + (-1)^{n-1} \cdot (-1)^n = t^n - 1, \end{aligned}$$

and $\{1, \xi_n, \xi_n^2, \dots, \xi_n^{n-1}\}$ are exactly the eigenvalues of σ . Now, consider the combinatorial set

$$Y := \left\{ y_{e_i} = \sum_{j=1}^n \xi_n^{(i-1)(j-1)} \cdot x_{\sigma^{j-1}(e_i)} \mid 1 \leq i \leq n \right\}.$$

Note that Y is a K -basis of V since the coefficients of each y_{e_i} are just different powers of the primitive root of unity ξ_n , and $\{x_{\sigma^{j-1}(e_i)} \mid 1 \leq j \leq n\} = X$ is a K -basis of V itself.

Let $i \in \{1, \dots, n\}$, then we easily compute that $\sigma(y_{e_i}) = \xi_n^{i-1} \cdot y_{e_i}$. Consequently, y_i is the eigenvector corresponding to the eigenvalue ξ_n^{i-1} , and the representation matrix $M(\sigma, Y)$ of $\sigma \in \text{Aut}(V)$ with respect to Y is diagonal.

Now, let $\sigma \in \mathbb{S}_n$ have cycle type $(l_1, \dots, l_{\vartheta(\sigma)})$ with cycle decomposition $\sigma = \sigma_1 \cdots \sigma_{\vartheta(\sigma)}$ and $\sigma_m = (e_{m,1} \dots e_{m,l_m})$ for $1 \leq m \leq \vartheta(\sigma)$. Then we have $\text{ord}(\sigma) = k = \text{lcm}(l_1, \dots, l_{\vartheta(\sigma)})$, $\text{ord}(\sigma_m) = l_m$, and

$$\xi_{l_m} = \xi_k^{k/l_m} \in K$$

is an l_m -th primitive root of unity. We set $X_m = \{x_{e_m,1}, \dots, x_{e_m,l_m}\}$ such that $\sigma_m \in \text{Aut}(V_m)$ with $V_m = \langle X_m \rangle_K$, and $X = X_1 \cup \dots \cup X_{\vartheta(\sigma)}$ is a K -basis of $V = V_1 \oplus \dots \oplus V_{\vartheta(\sigma)}$. Analogously to the n -cycle case we obtain the combinatorial sets

$$Y_m := \left\{ y_{e_m,i} = \sum_{j=1}^{l_m} \xi_{l_i}^{(i-1)(j-1)} \cdot x_{\sigma_m^{j-1}(e_m,1)} \mid 1 \leq i \leq l_m \right\}$$

of eigenvectors of $\sigma_m \in \text{Aut}(V_m)$ so that the representation matrix $M(\sigma_m, Y_m)$ of $\sigma_m \in \text{Aut}(V_m)$ with respect to the K -basis Y_m of V_m is diagonal with eigenvalues $\{1, \xi_{l_m}, \xi_{l_m}^2, \dots, \xi_{l_m}^{l_m-1}\}$. Hence, $Y = Y_1 \cup \dots \cup Y_{\vartheta(\sigma)}$ is a K -basis of V , consists of eigenvectors of $\sigma \in \text{Aut}(V)$, and the representation matrix

$$M(\sigma, Y) = \begin{pmatrix} M(\sigma_1, Y_1) & & \\ & \ddots & \\ & & M(\sigma_{\vartheta(\sigma)}, Y_{\vartheta(\sigma)}) \end{pmatrix} \in \text{Mat}(n \times n, K)$$

of $\sigma \in \text{Aut}(V)$ with respect to Y is diagonal with eigenvalues $\{\xi_{l_m}^j \mid 1 \leq m \leq \vartheta(\sigma), 0 \leq j \leq l_m - 1\} = \{\xi_k^{(k/l_m)j} \mid 1 \leq m \leq \vartheta(\sigma), 0 \leq j \leq l_m - 1\}$. \square

Remark 3.3. Due to the constructive proof of Proposition 3.2 the eigenvectors of $\sigma \in \text{Aut}(V)$ can be obtained purely combinatorial which is quite profitable from the algorithmic point of view. Hence, let us define the ring homomorphism

$$\tau : K[X] \longrightarrow K[X]$$

$$x_{e_m,i} \longmapsto y_{e_m,i} = \sum_{j=1}^{l_m} \xi_{l_i}^{(i-1)(j-1)} \cdot x_{\sigma_m^{j-1}(e_m,i)}$$

which maps the ring-variables onto the eigenvectors of $\sigma \in \text{Aut}(V)$. Consequently, we can define another ring-homomorphism σ_τ induced by the ring-automorphism $\sigma \in \text{Aut}(K[X])$ and the linear transformation $\tau \in \text{Aut}(K[X])$ obtained by the commutative diagram

$$\begin{array}{ccc} K[X] & \xrightarrow{\sigma} & K[X] \\ \downarrow \tau & & \downarrow \tau \\ K[X] & \xrightarrow{\sigma_\tau} & K[X] \end{array}$$

so that $\sigma_\tau = \tau \sigma \tau^{-1}$ satisfies the property that $\sigma_\tau(x_i) = \xi_k^{\nu_i} \cdot x_i$ for suitable exponents $0 \leq \nu_i \leq k-1$ and all $1 \leq i \leq n$.

Example 3.4. Let $\sigma = (12)(3) \in \mathbb{S}_3$ with $\text{ord}(\sigma) = 2$. Then consider $\xi_2 = -1 \in \mathbb{Q}$ and construct

$$\begin{aligned} \tau : \mathbb{Q}[x, y, z] &\longrightarrow \mathbb{Q}[x, y, z] \\ x &\longmapsto (-1)^{0 \cdot 0} \cdot x + (-1)^{0 \cdot 1} \cdot y = x + y, \\ y &\longmapsto (-1)^{1 \cdot 0} \cdot y + (-1)^{1 \cdot 1} \cdot x = y - x, \\ z &\longmapsto z \end{aligned}$$

as in Remark 3.3. Hence, τ is bijective with inverse τ^{-1} defined by

$$\tau^{-1}(x) = \frac{x-y}{2}, \quad \tau^{-1}(y) = \frac{x+y}{2}, \quad \tau^{-1}(z) = z.$$

Referring to Remark 3.3 σ_τ is induced by $\sigma_\tau = \tau\sigma\tau^{-1}$ and thus it holds

$$\begin{aligned}\sigma_\tau(x) &= \tau\sigma\tau^{-1}(x) = \tau\sigma\left(\frac{x-y}{2}\right) = \tau\left(\frac{y-x}{2}\right) = \frac{y-x-x+y}{2} = -x, \\ \sigma_\tau(y) &= \tau\sigma\tau^{-1}(y) = \tau\sigma\left(\frac{x+y}{2}\right) = \tau\left(\frac{x+y}{2}\right) = \frac{x+y+(y-x)}{2} = y, \\ \sigma_\tau(z) &= \tau\sigma\tau^{-1}(z) = \tau\sigma(z) = \tau(z) = z.\end{aligned}$$

Notation 3.5. For a better understanding we will index objects that live on the transformed side by τ .

As aforementioned respectively proven above, the induced automorphism σ_τ has a nice multiplication property on the ring variables what, however, is a priori not a sufficient reason for a fast Gröbner basis computation. But, in addition, the linear transformation τ also respects the symmetry of the input ideal.

Proposition 3.6. *If the ideal $I \subseteq K[X]$ is σ -symmetric, then the transformed ideal $I_\tau := \tau(I) \in K[X]$ is σ_τ -symmetric.*

Proof. Let $I = \langle f_1, \dots, f_r \rangle$. By definition of σ_τ we obtain for $\sigma(f_i) = f_j$ that $\sigma_\tau(\tau(f_i)) = \tau(\sigma(f_i)) = \tau(f_j)$. Thus, the ideal $I_\tau := \tau(I) = \langle \tau(f_1), \dots, \tau(f_r) \rangle$ is σ_τ -symmetric. \square

Example 3.7. Let $>=>_{dp}$ be the degree reverse lexicographical ordering¹, and $\sigma, \tau, \sigma_\tau$ as in Example 3.4. Now we consider the σ -symmetric ideal

$$I = \langle x^2y^2 - z, xy - 2y + 3z, xy - 2x + 3z \rangle \subseteq \mathbb{Q}[x, y, z]$$

and obtain that the transformed ideal

$$\begin{aligned}I_\tau := \tau(I) &= \langle x^4 - 2x^2y^2 + y^4 - z, -x^2 + y^2 + 2x - 2y + 3z, \\ &\quad -x^2 + y^2 - 2x - 2y + 3z \rangle \subseteq \mathbb{Q}[x, y, z]\end{aligned}$$

is σ_τ -symmetric.

Due to Proposition 3.2 and Proposition 3.6 we see that transforming the original ideal via τ still respects some symmetry. In particular, the ideal I_τ is σ_τ -symmetric and applying the automorphism σ_τ on any variable respectively monomial effects just a multiplication by a power of a primitive root of unity. The advantage of this circumstance is the fact that the symmetry propagates during the process of computing a Gröbner basis of I_τ which influences the performance in a positive way. More precisely, the following proposition holds.

Proposition 3.8. *Let I_τ be σ_τ -symmetric, then a Gröbner basis G_τ of I_τ satisfies $\sigma_\tau(g_\tau) = \xi_k^{\nu_{g_\tau}} \cdot g_\tau$ for all $g_\tau \in G_\tau$ with suitable $0 \leq \nu_{g_\tau} \leq k-1$.*

Proof. Let $I_\tau = \langle F_{I_\tau} \rangle$ and $f, g \in F_{I_\tau}$. Due to the property of σ_τ we can define $X^\alpha := \text{LM}(f) = \text{LM}(\sigma_\tau(f))$, $X^\beta := \text{LM}(g) = \text{LM}(\sigma_\tau(g))$, $X^\gamma := \text{lcm}(X^\alpha, X^\beta)$ and $\sigma_\tau(X^\alpha) = \xi_k^{\nu_\alpha} X^\alpha$, $\sigma_\tau(X^\beta) = \xi_k^{\nu_\beta} X^\beta$, $\sigma_\tau(X^\gamma) = \xi_k^{\nu_\gamma} X^\gamma$ for suitable $\nu_\alpha, \nu_\beta, \nu_\gamma \in \{0, \dots, k-1\}$. Then

$$\text{spoly}(f, g) = X^{\gamma-\alpha} \cdot f - \frac{\text{LC}(f)}{\text{LC}(g)} \cdot X^{\gamma-\beta} \cdot g$$

¹*Degree reverse lexicographical ordering:* Let $X^\alpha, X^\beta \in \text{Mon}(X)$. $X^\alpha >_{dp} X^\beta \iff \deg(X^\alpha) > \deg(X^\beta)$ or $(\deg(X^\alpha) = \deg(X^\beta) \text{ and } \exists 1 \leq i \leq n : \alpha_n = \beta_n, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i)$, where $\deg(X^\alpha) = \alpha_1 + \dots + \alpha_n$; cf. [GP07].

and again by the property of σ_τ it holds $\text{LC}(\sigma_\tau(f)) = \xi_k^{\nu_\alpha} \cdot \text{LC}(f)$ respectively $\text{LC}(\sigma_\tau(g)) = \xi_k^{\nu_\beta} \cdot \text{LC}(g)$. Thus

$$\begin{aligned} \sigma_\tau(\text{spoly}(f, g)) &= \sigma_\tau(X^{\gamma-\alpha}) \cdot \sigma_\tau(f) - \frac{\text{LC}(f)}{\text{LC}(g)} \cdot \sigma_\tau(X^{\gamma-\beta}) \cdot \sigma_\tau(g) \\ &= \xi_k^{\nu_\gamma - \nu_\alpha} \cdot X^{\gamma-\alpha} \cdot \sigma_\tau(f) - \frac{\text{LC}(f)}{\text{LC}(g)} \cdot \xi_k^{\nu_\gamma - \nu_\beta} \cdot X^{\gamma-\beta} \cdot \sigma_\tau(g) \\ &= \xi_k^{\nu_\gamma - \nu_\alpha} \cdot \left(X^{\gamma-\alpha} \cdot \sigma_\tau(f) - \frac{\text{LC}(f)}{\text{LC}(g)} \cdot \xi_k^{\nu_\alpha - \nu_\beta} \cdot X^{\gamma-\beta} \cdot \sigma_\tau(g) \right) \\ &= \xi_k^{\nu_\gamma - \nu_\alpha} \cdot \left(X^{\gamma-\alpha} \cdot \sigma_\tau(f) - \frac{\text{LC}(\sigma_\tau(f))}{\text{LC}(\sigma_\tau(g))} \cdot X^{\gamma-\beta} \cdot \sigma_\tau(g) \right) \\ &= \xi_k^{\nu_\gamma - \nu_\alpha} \cdot \text{spoly}(\sigma_\tau(f), \sigma_\tau(g)). \end{aligned}$$

Moreover, there are $a_h, r \in K[X]$ such that $\text{spoly}(f, g) = \sum_{h \in F_{I_\tau}} a_h h + r$. Due to the above computation it follows

$$\text{spoly}(\sigma_\tau(f), \sigma_\tau(g)) = \xi_k^{\nu_\alpha - \nu_\gamma} \cdot \sigma_\tau \left(\sum_{h \in F_{I_\tau}} a_h h + r \right) = \sum_{h \in F_{I_\tau}} b_h h + \xi_k^{\nu_\alpha - \nu_\gamma} \cdot \sigma_\tau(r),$$

for suitable $b_h = \xi_k^{\nu_\alpha - \nu_\gamma} \cdot a_{\sigma_\tau^{-1}(h)} \in K[X]$ since I_τ respectively F_{I_τ} is σ_τ -symmetric and consequently

$$\text{NF}(\text{spoly}(\sigma_\tau(f), \sigma_\tau(g)), F_{I_\tau}) = \xi_k^{\nu_\alpha - \nu_\gamma} \cdot \sigma_\tau(\text{NF}(\text{spoly}(f, g), F_{I_\tau})).$$

This property implies that the reduced Gröbner basis $G_\tau = \{g_1^\tau, \dots, g_s^\tau\}$ of I_τ satisfies $\sigma_\tau(g_i^\tau) = \xi_k^{\nu_{ij}} \cdot g_j^\tau$ for suitable $i, j \in \{1, \dots, s\}$ and $\nu_{ij} \in \{0, \dots, k-1\}$. Moreover, it follows $\text{LM}(g_i^\tau) = \text{LM}(\sigma_\tau(g_i^\tau)) = \text{LM}(g_j^\tau)$, but since G_τ is reduced we conclude $g_i^\tau = g_j^\tau$. Hence, we have $\sigma_\tau(g_i^\tau) = \xi_k^{\nu_i} \cdot g_i^\tau$ for all $i \in \{1, \dots, s\}$ with suitable $\nu_i \in \{0, \dots, k-1\}$. \square

Example 3.9. Let $I_\tau = \langle x^4 - 2x^2y^2 + y^4 - 16z, x^2 - y^2 - 4x + 4y + 12z, x^2 - y^2 - 4x - 4y + 12z \rangle \subseteq \mathbb{Q}[x, y, z]$ and $\sigma_\tau \in \text{Aut}(\mathbb{Q}[x, y, z])$ as obtained in Example 3.7. Then I_τ is σ_τ -symmetric, and its Gröbner basis

$$G_\tau = \{x, 12yz - 9z^2 - 8y + 13z, y^2 - 2y + 3z, 81z^3 + 36z^2 - 56y + 115z\}$$

satisfies $\sigma_\tau(g_\tau) = (-1)^{\nu_{g_\tau}} \cdot g_\tau$ for suitable $\nu_{g_\tau} \in \{1, 2\}$ and all $g_\tau \in G_\tau$. Now, the reverse transformation of G_τ yields the set

$$\begin{aligned} \tau^{-1}(G_\tau) &= \left\{ \frac{1}{2}x - \frac{1}{2}y, 6xz + 6yz - 9z^2 - 4x - 4y + 13z, \right. \\ &\quad \left. \frac{1}{4}x^2 + \frac{1}{2}xy + \frac{1}{4}y^2 - x - y + 3z, 81z^3 + 36z^2 - 28x - 28y + 115z \right\}. \end{aligned}$$

Obviously, just pulling back the Gröbner basis G_τ via τ^{-1} does not lead to a Gröbner basis of the input ideal I . Thus, we have to compute a Gröbner basis of the ideal $\langle \tau^{-1}(G_\tau) \rangle$ as well. Nevertheless, the advantage of this computation is the fact that the achieved property as described in Proposition 3.8 is respected by applying τ^{-1} on G_τ . More precisely, the following proposition holds.

Proposition 3.10. $\sigma(g) = \xi_k^{\nu_g} \cdot g$ for all $g \in \tau^{-1}(G_\tau)$ and suitable $0 \leq \nu_g \leq k-1$.

Proof. Let $g \in \tau^{-1}(G_\tau)$, i.e. there is an $g_\tau \in G_\tau$ such that $g = \tau^{-1}(g_\tau)$. Then due to Proposition 3.2 and Proposition 3.8 we have

$$\tau(\sigma(g)) = \tau(\sigma(\tau^{-1}(g_\tau))) = \sigma_\tau(g_\tau) = \xi_k^{\nu_{g_\tau}} \cdot g_\tau$$

for some $\nu_{g_\tau} \in \{0, \dots, k-1\}$. Hence, we obtain

$$\sigma(g) = \tau^{-1}(\tau(\sigma(g))) = \tau^{-1}(\xi_k^{\nu_{g_\tau}} \cdot g_\tau) = \xi_k^{\nu_{g_\tau}} \cdot \tau^{-1}(g_\tau) = \xi_k^{\nu_{g_\tau}} \cdot g.$$

This proves the proposition. \square

Example 3.11. Let $\sigma = (12)(3) \in \mathbb{S}_3$ with $\text{ord}(\sigma) = 2$, $\xi_2 = -1 \in \mathbb{Q}$ and $\tau^{-1}(G_\tau)$ as obtained in Example 3.9. Then we compute

$$\begin{aligned} \sigma\left(\frac{1}{2}x - \frac{1}{2}y\right) &= -\left(\frac{1}{2}x - \frac{1}{2}y\right), \\ \sigma(6xz + 6yz - 9z^2 - 4x - 4y + 13z) &= 6xz + 6yz - 9z^2 - 4x - 4y + 13z, \\ \sigma\left(\frac{1}{4}x^2 + \frac{1}{2}xy + \frac{1}{4}y^2 - x - y + 3z\right) &= \frac{1}{4}x^2 + \frac{1}{2}xy + \frac{1}{4}y^2 - x - y + 3z, \\ \sigma(81z^3 + 36z^2 - 28x - 28y + 115z) &= 81z^3 + 36z^2 - 28x - 28y + 115z, \end{aligned}$$

as claimed in Proposition 3.10.

The following diagram summarizes and illustrates our way of improving the computation of a Gröbner basis G of a σ -symmetric ideal I .

$$\begin{array}{ccc} (I, \sigma) & \xrightarrow{\tau} & (I_\tau, \sigma_\tau) \\ & & \downarrow \text{std} \\ \langle \tau^{-1}(G_\tau) \rangle & \xleftarrow{\tau^{-1}} & G_\tau \\ & & \downarrow \text{std} \\ & & G \end{array}$$

Note that the linear transformation τ is defined in Remark 3.3 and the procedure **std** is implemented in SINGULAR and computes a Gröbner basis respectively standard basis of the input.

Algorithm 1 computes the Gröbner basis of a σ -symmetric ideal I .²

Algorithm 1 Symmetric Gröbner Basis Computation (**symmStd**)

Input: $I \subseteq K[X]$, $\sigma \in \mathbb{S}_n$ such that I is σ -symmetric.

Output: $G \subseteq K[X]$ the Gröbner basis of I .

- 1: $k := \text{ord}(\sigma)$;
 - 2: **if** $(k \bmod \text{char}(K) = 0)$ **then**
 - 3: **print** Warning, algorithm is not applicable.
 - 4: **return** \emptyset ;
 - 5: **if** $(k = 2 \text{ or } (\text{char}(K) - 1) \bmod k = 0)$ **then**
 - 6: compute $\xi_k \in K$;
 - 7: **else**
 - 8: $K = K[a]/\Phi_k(a)$;
 - 9: $\xi_k := a$;
 - 10: compute $\tau \in \text{Aut}(K[X])$;
 - 11: compute a Gröbner basis G_τ of $I_\tau = \tau(I)$;
 - 12: compute a Gröbner basis G of $\langle \tau^{-1}(G_\tau) \rangle$;
 - 13: **return** G ;
-

²The corresponding procedures are implemented in SINGULAR in the library **symodstd.lib**.

Theorem 3.12. *Algorithm 1 terminates and is correct, i.e. the output G is a Gröbner basis of the input I .*

Proof. Termination is clear and for proving correctness it suffices to show that $I = \langle \tau^{-1}(G_\tau) \rangle$ since G is by definition a Gröbner basis of $\langle \tau^{-1}(G_\tau) \rangle$. Let $f \in I$ and $G_\tau = \{g_1^\tau, \dots, g_s^\tau\}$. Then $\tau(f) \in \tau(I) = I_\tau$ and consequently there are $a_1, \dots, a_s \in K[X]$ such that $\tau(f) = \sum_{i=1}^s a_i \cdot g_i^\tau$ since G_τ is a Gröbner basis of I_τ . Hence, we obtain

$$f = \tau^{-1}(\tau(f)) = \sum_{i=1}^s \tau^{-1}(a_i) \cdot \tau^{-1}(g_i^\tau) \in \langle \tau^{-1}(G_\tau) \rangle.$$

For the other inclusion let $g \in \langle \tau^{-1}(G_\tau) \rangle$. It follows that $\tau(g) \in \langle G_\tau \rangle = I_\tau = \tau(I)$ and moreover $g \in I$ since τ is an automorphism. \square

For illustration of Algorithm 1 we combine all previous examples.

Example 3.13. Again, let $I = \langle x^2y^2 - z, xy - 2y + 3z, xy - 2x + 3z \rangle \subseteq \mathbb{Q}[x, y, z]$ and $\sigma = (12)(3) \in \mathbb{S}_3$. Referring to Examples 3.4, 3.7, 3.9 and 3.11 we already obtained

$$I_\tau := \tau(I) = \langle x^4 - 2x^2y^2 + y^4 - z, -x^2 + y^2 + 2x - 2y + 3z, \\ -x^2 + y^2 - 2x - 2y + 3z \rangle,$$

and its Gröbner basis

$$G_\tau = \{x, 12yz - 9z^2 - 8y + 13z, y^2 - 2y + 3z, 81z^3 + 36z^2 - 56y + 115z\}$$

with

$$\tau^{-1}(G_\tau) = \left\{ \frac{1}{2}x - \frac{1}{2}y, 6xz + 6yz - 9z^2 - 4x - 4y + 13z, \right. \\ \left. \frac{1}{4}x^2 + \frac{1}{2}xy + \frac{1}{4}y^2 - x - y + 3z, 81z^3 + 36z^2 - 28x - 28y + 115z \right\}.$$

Finally, we compute

$$G = \{x - y, 12yz - 9z^2 - 8y + 13z, y^2 - 2y + 3z, 81z^3 + 36z^2 - 56y + 115z\},$$

the Gröbner basis of $\langle \tau^{-1}(G_\tau) \rangle$ respectively I .

Remark 3.14. It is remarkable that we even achieve an advancement although we have to compute Gröbner bases internally twice on modified input ideals via `std` (cf. Section 5).

4. COMPUTING GRÖBNER BASES USING SYMMETRY AND MODULAR METHODS

When applying Algorithm 1 on σ -symmetric ideals over the rationals such that $\text{ord}(\sigma) = k > 2$ we need to swap to $\mathbb{Q}[a]/\Phi_k(a)$ as explained in Remark 3.1. However, over fields K of positive characteristic such that $k \mid (\text{char}(K) - 1)$ this can be omitted. Consequently, we use modular methods to improve Algorithm 1 applied on σ -symmetric ideals in the polynomial ring over the rationals. More precisely, we improve the modular Gröbner basis algorithm as introduced by Arnold (cf. [A03]) and Idrees, Pfister, Steidel (cf. [IPS11]).

Algorithm 2 combines the algorithms `symmStd` (cf. Algorithm 1) and `modStd` (cf. [IPS11, Algorithm 1]).³

Algorithm 2 Symmetric Modular Gröbner Basis Computation (`syModStd`)

Input: $I \subseteq \mathbb{Q}[X]$ and $\sigma \in \mathbb{S}_n$ such that I is σ -symmetric.

Output: $G \subseteq \mathbb{Q}[X]$ the Gröbner basis of I .

```

1:  $k := \text{ord}(\sigma)$ ;
2: choose  $P$ , a list of random primes such that  $k \mid (p - 1)$  for all  $p \in P$ ;
3:  $GP = \emptyset$ ;
4: loop
5:   for  $p \in P$  do
6:      $G_p = \text{symmStd}(I_p, \sigma)$ ;
7:      $GP = GP \cup \{G_p\}$ ;
8:    $(GP, P) = \text{deleteUnluckyPrimesSB}(GP, P)$ ;
9:   lift  $(GP, P)$  to  $G \subseteq \mathbb{Q}[X]$  by applying Chinese remainder and Farey rational
   map;
10:  if pTestSB( $I, G, P$ ) then
11:    if  $I \subseteq \langle G \rangle$  then
12:      if  $G$  is a standard basis of  $\langle G \rangle$  then
13:        return  $G$ ;
14:  enlarge  $P$ ;
```

Remark 4.1. The essential differences compared to the algorithm `modStd` are the following:

- (1) The choice of the prime list P has to be restricted. Every considered prime number $p \in P$ has to satisfy the condition $k \mid (p - 1)$ in order to assure that the coefficient field \mathbb{F}_p has a k -th primitive root of unity.
- (2) The modular Gröbner bases G_p are computed via `symmStd` instead of `std`.

Similar to `modStd` we can parallelize Algorithm 2 by computing the modular Gröbner bases G_p respectively performing the final tests in parallel.

Theorem 4.2. *Algorithm 2 terminates and is correct, i.e. the output G is a Gröbner basis of the input I .*

Proof. Termination is clear and correctness follows directly from Theorem 3.12 and [IPS11, Theorem 2.4]. \square

5. EXAMPLES AND TIMINGS

In this section we provide examples on which we time the new algorithms `symmStd` (cf. Section 3) respectively `syModStd` (cf. Section 4) and its parallelization as opposed to the former algorithms `std` respectively `modStd` implemented in SINGULAR. Timings are conducted by using SINGULAR 3-1-3 on an AMD Opteron 6174 machine with 48 CPUs, 2.2 GHz, and 128 GB of RAM running the Gentoo Linux operating system.

³The corresponding procedures are implemented in SINGULAR in the library `symodstd.lib`.

Example 5.1 (Cyclic n -roots (cf. [Bj85], [Bj90], [BF91])). The task to compute a Gröbner basis of the ideal in $\mathbb{Q}[X] = \mathbb{Q}[x_1, \dots, x_n]$ corresponding to the following system of polynomial equations

$$\begin{aligned} x_1 + \dots + x_n &= 0 \\ x_1x_2 + x_2x_3 + \dots + x_{n-1}x_n + x_nx_1 &= 0 \\ &\vdots \\ x_1x_2 \cdots x_{n-1} + x_2x_3 \cdots x_n + \dots + x_{n-1}x_n \cdots x_{n-3} + x_nx_1 \cdots x_{n-2} &= 0 \\ x_1 \cdots x_n - 1 &= 0 \end{aligned}$$

has become a benchmark problem for Gröbner basis techniques. We call this ideal *cyclic*(n), and its variety *cyclic n -roots* (cf. [Bj85]). The origin of the problem is related to Fourier analysis (cf. [Bj85], [Bj90]). Obviously, the ideal *cyclic*(n) is by definition symmetric with respect to the n -cycle $\sigma_n = (1 \dots n)$ such that we can apply the algorithms `symmStd` and `syModStd`.

Until the end of 2009, SINGULAR was able to compute a Gröbner basis of *cyclic*(n) for $n \leq 8$. In April 2010, we could for the first time compute a Gröbner basis of *cyclic*(9) via a prototype of `syModStd` by using the 32-bit version of SINGULAR 3-1-1 on an Intel® Xeon® X5460 machine with 4 CPUs, 3.16 GHz each, and 64 GB of RAM under the Gentoo Linux operating system within 23 days.

Table 1 summarizes the present timings for computing a Gröbner basis of *cyclic*(n) for $n = 7, 8, 9$ with different numbers of cores ℓ denoted by `modStd`(ℓ) respectively `syModStd`(ℓ), and different permutations σ where again $k = \text{ord}(\sigma)$ denotes the order of σ .

n	k	<code>symmStd</code>	<code>modStd</code> (1)	<code>modStd</code> (30)	<code>syModStd</code> (1)	<code>syModStd</code> (30)
7	7	409.394	106	38	165	50
8	2	-	6.816	973	5.196	811
8	4	-	6.816	973	3.120	620
8	8	-	6.816	973	4.454	788
9	9	-	9.935.103	475.981	2.790.303	207.681

TABLE 1. Total running times in seconds for computing a Gröbner basis of *cyclic*(n) for $n = 7, 8, 9$ via `symmStd`, `modStd`(ℓ), and `syModStd`(ℓ) for $\ell = 1, 30$, using different permutations of order k . The symbol “-” indicates out of memory failures.

In these examples we used the permutation $(1234567) \in \mathbb{S}_7$ for $n = 7$, the permutations $(18)(27)(36)(45), (1753)(2864), (12345678) \in \mathbb{S}_8$ for $n = 8$, and the permutation $(147)(258)(369) \in \mathbb{S}_9$ for $n = 9$. Note that the timings obtained by the modular versions are dependent on the used permutation and especially on its order. In particular, a higher order k , that is a higher symmetry, speeds up the Gröbner basis computation on the transformed side but in contrast slows down the application of the linear transformation τ (cf. Remark 3.3) since the support of a ring-variable’s image depends on the order k of the permutation. This circumstance justifies that applying the symmetric modular algorithm for computing a Gröbner basis of *cyclic*(8) is most performant when using the permutation $(1753)(2864) \in \mathbb{S}_8$ of order 4.

Example 5.2 (100 Swiss Francs Problem (cf. [ZJG11], [St08])). B. Sturmfels offered a cash prize of 100 Swiss Francs for the resolution of a very specific conjecture in the *Nachdiplomsvorlesung* (postgraduate course) which he held at ETH Zürich in the summer of 2005. Based on a concrete biological example proposed in [PS05, Example 1.16] the problem arised to maximize the likelihood function

$$L(P) = \left(\prod_{i=1}^4 p_{ii} \right)^4 \cdot \left(\prod_{i \neq j} p_{ij} \right)^2 \cdot \left(\sum_{i,j=1}^4 p_{ij} \right)^{-40}$$

over all (positive) 4×4 - matrices $P = (p_{ij})_{1 \leq i,j \leq 4}$ of rank at most two. Due to numerical experiments by applying an expectation-maximization algorithm (EM algorithm), B. Sturmfels conjectured that the matrix

$$P = \frac{1}{40} \begin{pmatrix} 3 & 3 & 2 & 2 \\ 3 & 3 & 2 & 2 \\ 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 3 \end{pmatrix}$$

is a global maximum of the likelihood function $L(P)$ (cf. [St08]).

The conjecture is positively confirmed in [ZJG11]. In their approach via Gröbner bases (cf. [ZJG11, Section 2.3]) it is necessary to compute the Gröbner basis of the ideal J defined by

$$I = \left\langle a_1 - b_1, \sum_{i=1}^4 a_i, \sum_{i=1}^4 b_i, f_1, \dots, f_4, g_1, \dots, g_4 \right\rangle \subseteq \mathbb{Q}[a_1, \dots, a_4, b_1, \dots, b_4]$$

with

$$\begin{aligned} f_i &= \sum_{j=1}^4 \left(b_j \cdot (1 + a_i b_i) \cdot \prod_{k \neq j} (1 + a_i b_k) \right) + b_i \cdot \prod_{k=1}^4 (1 + a_i b_k) \\ g_i &= \sum_{j=1}^4 \left(a_j \cdot (1 + a_i b_i) \cdot \prod_{k \neq j} (1 + a_k b_i) \right) + a_i \cdot \prod_{k=1}^4 (1 + a_k b_i) \end{aligned}$$

for $1 \leq i \leq 4$, and

$$J = I + \langle 1 - u a_1 \rangle \subseteq \mathbb{Q}[a_1, \dots, a_4, b_1, \dots, b_4, u]$$

with respect to an elimination ordering on the variable u . In a first approach we therefore applied `modStd` using the lexicographical ordering $>_{lp}$ respectively the block ordering $(>_{dp(8)}, >_{lp(1)})$ to eliminate the variable u . It turned out that both variants are comparably slow so that we used in a second approach the degree reverse lexicographical ordering $>_{dp}$, and applied the FGLM-algorithm (cf. [FGLM93]) subsequently to obtain a Gröbner basis with respect to the block ordering $(>_{dp(8)}, >_{lp(1)})$. Since the ideal $J \subseteq \mathbb{Q}[a_1, \dots, a_4, b_1, \dots, b_4, u]$ is symmetric with respect to the permutation $(34)(78) \in \mathbb{S}_9$ we could moreover apply the algorithm `syModStd`. The timings for the computations in SINGULAR are summarized in Table 2.

Method	Running Time
<code>modStd</code> [$>_{lp}$]	39919
<code>modStd</code> [$(>_{dp(8)}, >_{lp(1)})$]	515
<code>syModStd</code> [$(>_{dp(8)}, >_{lp(1)})$]	356
<code>modStd</code> [$>_{dp}$] – <code>fglm</code> [$(>_{dp(8)}, >_{lp(1)})$]	375
<code>syModStd</code> [$>_{dp}$] – <code>fglm</code> [$(>_{dp(8)}, >_{lp(1)})$]	284

TABLE 2. Total running times in seconds for computing the Gröbner basis of $J \subseteq \mathbb{Q}[a_1, \dots, a_4, b_1, \dots, b_4, u]$ with respect to an elimination ordering on the variable u via different methods.

Example 5.3 (Inverse Galois Problem (cf. [Mal94], [Mat87], [MM99])). A major topic in algebraic number theory is the inverse Galois problem over a field K , i.e. the question whether any finite group G is the Galois group of a Galois extension of K . The most interesting case is $K = \mathbb{Q}$ which is still open in general. In contrast, the problem is known to be true for K being a rational function field in one variable t over an algebraically closed field of characteristic zero. In particular, it is true for $K = \mathbb{C}(t)$, and in this case it is solved via geometric field extensions (see for example [MM99, I, §1]). Moreover, the same strategy applies to finite field extensions of $\overline{\mathbb{Q}}(t)$ ramified only over $\{0, 1, \infty\}$ (see for example [MM99, I, §5]). In this situation, for any triple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ of elements generating a transitive subgroup $G = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \subseteq \mathbb{S}_n$ with $\sigma_1 \sigma_2 \sigma_3 = 1$ there exists a certain field extension $\overline{K}_\sigma / \overline{\mathbb{Q}}(t)$ of degree n , unramified outside $\{0, 1, \infty\}$, and whose Galois group is isomorphic to G . In fact, any such extension $\overline{K}_\sigma / \overline{\mathbb{Q}}(t)$ is already defined over a number field $k_\sigma = \mathbb{Q}(\alpha_\sigma)$, the so-called field of definition of $\overline{K}_\sigma / \overline{\mathbb{Q}}(t)$, so that there exists a further field extension $K_\sigma / k_\sigma(t)$ which also has G as its Galois group. The degree $[k_\sigma : \mathbb{Q}]$ is bounded from above by group theoretical information (see for example [Mal94, Proposition A]). In order to construct the extension $\overline{K}_\sigma / \overline{\mathbb{Q}}(t)$ it is necessary to solve a system of polynomial equations (see [MM99, I, §9]). In case that, for example, σ_1 and σ_2 have the same cycle type, the defining ideal is symmetric with respect to a permutation of order 2 so that we can apply the algorithms `symmStd` and `syModStd` to compute a Gröbner basis of this system. In addition, choosing an elimination ordering for the last ring variable, the last polynomial f of the Gröbner basis of this system of non-linear equations generates the field of definition $k_\sigma = \mathbb{Q}(\alpha_\sigma)$ insofar that α_σ is a zero of f . The irreducible factors of f together with group theoretical information yield restrictions on $[k_\sigma : \mathbb{Q}]$. In case that $[k_\sigma : \mathbb{Q}] = 1$, the given group G can even be realized over $\mathbb{Q}(t)$, and therefore also over \mathbb{Q} by Hilbert's irreducibility theorem.

In 1994, G. Malle collected computational data on several k_σ of degree $[k_\sigma : \mathbb{Q}] \leq 13$ (cf. [Mal94]) with the intention to observe regularities and hints to decrease the group theoretical bound. Table 3 lists further examples in the spirit of this article and which could not be computed at that time.

Note that all ideals belonging to the examples listed in Table 3 are zero-dimensional such that we can compute a Gröbner basis with respect to the degree reverse lexicographical ordering, and obtain a lexicographical Gröbner basis by applying the FGLM-algorithm (cf. [FGLM93]) subsequently.

n	G	C_σ	$[k_\sigma : \mathbb{Q}]$	symmStd	modStd	syModStd
7	\mathbb{A}_7	$4.2 - 4.2 - 4.2$	12	24	19	19
9	\mathbb{S}_9	$4.2^2 - 4.2^2 - 5.3$	34	5	15	13
10	\mathbb{A}_{10}	$5.2^2 - 5.2^2 - 7$	37	977	186	107
11	\mathbb{A}_{11}	$4.2 - 9 - 9$	12	17	2	1
11	\mathbb{A}_{11}	$4.2 - 4^2.3 - 4^2.3$	8	34	3	2
11	\mathbb{A}_{11}	$4.2 - 5.3^2 - 5.3^2$	8	15	3	2
11	\mathbb{A}_{11}	$5 - 8.2 - 8.2$	11	265	17	8
11	\mathbb{A}_{11}	$5 - 6.4 - 6.4$	11	339	20	10
11	\mathbb{A}_{11}	$5 - 7.3 - 7.3$	11	292	16	8
11	\mathbb{S}_{11}	$7 - 4.3^2 - 4.3^2$	26	631245	2506	1493
11	\mathbb{S}_{11}	$7 - 4.3.2^2 - 4.3.2^2$	29	-	3039	1979
11	\mathbb{S}_{11}	$7 - 7.2 - 7.2$	29	-	1414	702
11	\mathbb{S}_{11}	$7 - 5.4 - 5.4$	26	-	1738	899

TABLE 3. Total running times in seconds for computing the defining Gröbner basis of the field extension $\overline{K}_\sigma/\mathbb{Q}(t)$ having group G and conjugacy class triple C_σ (cf. [Mal94]) via **symmStd**, **modStd**, and **syModStd**. Here, C_σ is a class of G containing elements of the given cycle type. The symbol “-” indicates out of memory failures.

Conclusion 5.4. In all considered examples the symmetric modular version of the Gröbner basis algorithm is the most performant one, and is, hence, a quite powerful tool if the input ideal is symmetric with respect to some permutation of the ring-variables.

6. ACKNOWLEDGEMENT

The author would like to thank his supervisors Gunter Malle and Gerhard Pfister for introducing to the topic of this article and constant support. In addition, he thanks Michael Cuntz, Christian Eder and Ulrich Thiel for helpful discussions.

REFERENCES

- [A03] Arnold, E. A.: Modular algorithms for computing Gröbner bases. *Journal of Symbolic Computation* 35, 403–419 (2003).
- [Bj85] Björck, G.: Functions of modulus on Z_p whose Fourier transforms have constant modulus. *Proc. A. Haar Memorial Conference, Colloquia Mathematica Societatis János Bolyai* 49, Budapest, 193–197 (1985).
- [Bj90] Björck, G.: Functions of modulus on Z_n whose Fourier transforms have constant modulus, and “cyclic n -roots”. *Recent Advances in Fourier Analysis and its Applications* (J. S. Byrnes and J. F. Byrnes, eds.), NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci., Kluwer, 131–140 (1990).
- [BF91] Björck, G.; Fröberg, G.: A Faster Way to Count the Solution of Inhomogeneous Systems of Algebraic Equations, with Applications to Cyclic n -Roots. *Journal of Symbolic Computation* 12, 329–336 (1991).
- [Bu65] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *Dissertation, Innsbruck, Austria* (1965).
- [DGPS11] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: *SINGULAR 3-1-3 — A computer algebra system for polynomial computations*. <http://www.singular.uni-kl.de> (2011).

- [FGLM93] Faugère, J. C.; Gianni, P.; Lazard, D.; Mora, T.: Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation* 16, 329–344 (1993).
- [GP07] Greuel, G.-M.; Pfister, G.: *A SINGULAR Introduction to Commutative Algebra*. Second edition, Springer (2007).
- [IPS11] Idrees, N.; Pfister, G.; Steidel, S.: Parallelization of Modular Algorithms. *Journal of Symbolic Computation* 46, 672–684 (2011).
- [Mal94] Malle, G.: Fields of definition of some three point ramified field extensions. In: *The Grothendieck theory of dessins d'enfants*. London Mathematical Society Lecture Notes 200, Cambridge University Press, Cambridge, 147–168 (1994).
- [MM99] Malle, G.; Matzat, B. H.: *Inverse Galois Theory*. Springer (1999).
- [Mat87] Matzat, B. H.: *Konstruktive Galoistheorie*. Springer Lecture Notes in Mathematics 1284, (1987).
- [PS05] Pachter, L.; Sturmfels, B.: *Algebraic Statistics for Computational Biology*. Cambridge University Press, Cambridge (2005).
- [Se96] Serre, J.-P.: *Linear Representations of Finite Groups*. Graduate Texts in Mathematics 42, Springer (1996).
- [St08] Sturmfels, B.: Open problems in Algebraic Statistics. In: Putinar, M.; Sullivant, S. (eds.): *Emerging Applications of Algebraic Geometry*, I.M.A. Volumes in Mathematics and its Applications 149, Springer, New York, 351–364 (2008).
- [ZJG11] Zhu, M.; Jiang, G.; Gao, S.: Solving the 100 Swiss Francs Problem. *Mathematics in Computer Science* 5, 195–207 (2011).

STEFAN STEIDEL, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF KAISERSLAUTERN, ERWIN-SCHRÖDINGER-STR., 67663 KAISERSLAUTERN, GERMANY

E-mail address: `steidel@mathematik.uni-kl.de`

URL: `http://www.mathematik.uni-kl.de/~steidel`